The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB GOVERNMENT'S CONSOLIDATED RESPONSE TO DEFENDANT'S MOTION TO DISMISS AND REPLY REGARDING MOTION FOR RECONSIDERATION OF ORDER GRANTING DEFENDANT'S THIRD MOTION TO COMPEL AND FOR LEAVE TO SUBMIT RULE 16(d)(1) FILING *EX PARTE* AND *IN CAMERA* (Redacted Version)

I. INTRODUCTION

For at least three reasons, the Court should grant the government's motion for reconsideration of its discovery order and deny Michaud's motion to dismiss the indictment.

First, an *ex parte*/*in camera* proceeding is necessary for the government to fully articulate the basis of its assertion of a qualified law enforcement privilege. The government's previous decision to withdraw its request for that hearing was a misstep

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

that left this Court with an incomplete picture on which to base its decision. The government seeks to remedy this and provide the Court with the information necessary to fully assess its claim of privilege.

Second, Michaud persists in his refusal to explain how the discovery he seeks has any bearing on the questions he says remain unanswered. Michaud has all the tools he needs to verify the operation of the NIT on his computer and the accuracy of the information collected. And his suggestion that additional computer code would somehow shed light on his theory that someone or something else placed thousands of images of child pornography (organized into folders by category) on his thumb drive simply does not hold water. Michaud has all the tools he needs to answer the questions he poses and prepare his defense. The code used to deliver the NIT would add nothing. That reason alone justifies reconsideration here.

Finally, Michaud's request that the Court dismiss the indictment should be denied as premature. The need to resolve the question of what, if any, sanction should follow noncompliance with the Court's discovery order will arise only after the government's reconsideration motion has been resolved. Regardless, the drastic sanction of dismissal is unwarranted as a lesser sanction would address the issue of what Michaud received through the Playpen website.

II. ARGUMENT

A. Reconsideration is proper under the Local Rules.

Michaud argues that the Court should deny the motion for reconsideration, without regard to its merits, because the motion does not meet the procedural requirements under the Local Rules. Local Criminal Rule 12(b)(10)(A) states that "[t]he court will ordinarily deny such motions in the absence of a showing of manifest error . . . or a showing of new facts or legal authority which could not have been brought to its attention earlier with reasonable diligence."

The government has not alleged "manifest error" nor "new facts or legal authority" that could not have been brought to the Court's attention earlier. However, the

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Local Rule does not require courts to automatically reject all motions for reconsideration that fail to meet those criteria. Rather, the Rule says that such requests should "ordinarily" be denied. This is not an ordinary situation. [redacted]

In the Response to the Motion to Reconsider, the defense argues vehemently that *ex parte* proceedings are unfair and unjust. Response at pp. 15-16. The government does not accept all of those arguments, but the government does agree that *ex parte* proceedings are a last resort. Ideally, matters are litigated through the traditional adversary process. [redacted]

The government should not be punished for its well-meaning attempt to litigate this issue without an *ex parte* submission. The matters at stake are simply too important. Rather, the Court should find that the Motion to Reconsider is not the "ordinary" motion envisioned by Rule 12(b)(10)(A) and should address the Motion on its merits.

B. The defense's claim that the FBI has misled courts and prosecutors in other cases is inaccurate.

Before reaching the substantive arguments raised in the defense Response, it is important to clear away some smoke. The defense urges the Court to "discount[]" the government's arguments about the NIT and related technology because the FBI has—

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

supposedly—"misled courts in other cases" and improperly "conceal[ed] information about its NITs . . . from federal prosecutors and even its own case agents." Response at pp. 5-6.

This is an extraordinary allegation. The defense claims to have actual "evidence" showing that the FBI has deceived courts and prosecutors and that this "evidence" is so powerful that the Court should treat the FBI as an inherently untrustworthy organization and "discount" the information it provides out of hand. One would expect that such a claim would be supported by abundant, concrete evidence showing widespread deception and improper concealment. Instead, much of the "support" comes in the form of media reports and an anecdotal trial story. Furthermore, a careful reading of this material shows no evidence that the FBI has deceived or misled courts or prosecutors.

The centerpiece of Michaud's argument is the Maryland Court of Special Appeals decision in *State v. Andrews*, 2016 WL 1254567 (Md. Ct. Spec. App. March 30, 2016). According to the defense, *Andrews* is "evidence" that the FBI "has misled courts in other cases" about its technology. Response at p. 5. In truth, *Andrews* involved neither an FBI investigation nor a NIT. The investigating agency in *Andrews* was the Baltimore Police Department ("BPD"), the case was charged in state court, and the technology at issue was the warrantless use of cell phone tracking technology known as "Hailstorm." *Andrews*, 2016 WL 1254567 at *1.

In *Andrews*, local police and prosecutors used the "Hailstorm" tracking device pursuant to an order from a state court judge authorizing a pen/trap device pursuant to Maryland law. *Id.* at *13. The appellate court found that the application failed to adequately disclose the nature of the "Hailstorm" device and how it would be used in the investigation, and that the Fourth Amendment required a search warrant to authorize the use of "Hailstorm." *Id.* at *32-33.

Although the FBI was not involved in the investigation, the appellate court noted that the BPD had purchased the "Hailstorm" device from the FBI pursuant to a non-disclosure agreement. *Id.* at *11. In essence, the non-disclosure agreement prohibited

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

state prosecutors from disclosing information about "Hailstorm" in court filings or proceedings "without the prior written approval of the FBI." *Id.* The agreement also required the state prosecutors to notify the FBI if a court ordered disclosure of "Hailstorm" to provide the FBI "time to intervene" in the state case. *Id.*

The appellate court speculated—without citing to any evidence or anything in the record—that the non-disclosure agreement was what prevented state prosecutors from adequately disclosing "Hailstorm" in the pen/trap application. *Id.* at *12. There are a number of important things to note about the *Andrews* decision.

First, neither the FBI nor the DOJ were a party to the state court case, and thus neither was able to weigh in regarding the non-disclosure agreement and its role.

Second, the *Andrews* decision is not even final. It has not yet been published and remains "subject to revision or withdrawal." *Id.* (see caption).

Third, the FBI made no false or misleading statements to courts, prosecutors, or anybody else in the *Andrews* investigation. The pen/trap application and related statements in *Andrews* were made by local law enforcement and local prosecutors.

Fourth, Michaud's case does not involve a non-disclosure agreement, and the merits of that agreement are a red herring. Even in the context of *Andrews*, Michaud's claim that the non-disclosure agreement "obstructed" disclosure simply does not hold up to scrutiny. The non-disclosure agreement did not force the local prosecutors and police to make inaccurate statements or withhold information about "Hailstorm" from the state court. To the contrary, the agreement specifically authorized local law enforcement to approach the FBI and ask permission to make disclosures in the pen/trap application. If the FBI denied permission and local law enforcement believed that an application without those disclosures would be incomplete, local law enforcement could have decided not to submit the application. Nothing in *Andrews* suggests that local law enforcement asked the FBI for permission to disclose "Hailstorm." Furthermore, apart from the appellate court's unsupported speculation, there is no evidence that the non-disclosure agreement affected law enforcement's actions at all.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Indeed, the nondisclosure agreement allowed for the possibility that there might be a need to litigate discovery issues related to "Hailstorm," and sought notice to allow the FBI to intervene and state its position to a court. If in fact—as the *Andrews* court found—the pen/trap application failed to disclose material information, that failure must be laid at the feet of the prosecutors and police who handled the investigation.[1]

Fifth, Michaud claims that the non-disclosure agreement prohibited local police and prosecutors from disclosing information "even if ordered to do so by a court." Response at p. 5 (citing *Andrews*). Michaud's implication is that the non-disclosure agreement would force local prosecutors to act unethically. Again, this is refuted by the language of the agreement, which in fact requires law enforcement to notify the FBI to give it a chance to "intervene" in the case to protect its interests. *Andrews,* 2016 WL 1254567, at *12. The agreement also required local prosecutors to dismiss charges at the FBI's request if necessary to avoid disclosure, which is not an unethical or dishonest option.

Finally, the defense cites passionate language from the *Andrews* case and the United States Supreme Court about the importance of protecting people's privacy and the dangers of a surveillance state. Response at p. 7. These laudable statements are irrelevant to the issues in this Motion. This case does not involve "[w]iretapping and 'bugging' run rampant, without effective judicial or legislative control." *Andrews* at *10 (citation omitted). The NIT was delivered to Michaud's computer pursuant to a search warrant. The search warrant application disclosed all material information to the court that issued the warrant. Although this Court found a technical defect in the warrant, it denied suppression and found no improper government conduct.[2]

Having twisted *Andrews* beyond recognition to support the claim that the FBI deceived the court in that case, the defense moves on to allege other examples of

---

[1] To be clear, the government is not taking any position on the merits of *Andrews* or the propriety of the actions of the investigators in that case.

[2] The Supreme Court has now approved an amendment to Rule 41 that clarifies a magistrate's authority to issue a warrant to search computers outside of the issuing judge's District in cases such as this.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

misleading behavior by "agents" and improper "conceal[ment]" of information about "NITs and other surveillance technology." Response at pp. 5-6. As shown below, these allegations are equally baseless.

The defense cites articles published by The Guardian and Wired.com regarding alleged failures by the BPD and other local law enforcement agencies to adequately disclose "Stingray" (related to "Hailstorm") technology to courts and defense counsel. As an initial matter, these media reports – which are full of unproven claims by defense attorneys and advocates – are not proper proof of anything. In any event, the articles (which are attached as Exhibits A and B, respectively) deal with the actions of local law enforcement, and do not allege any false or misleading statements by the FBI to courts or defense counsel. *See* Ex. B (alleging that "*[l]ocal law enforcement agencies* . . . have even deceived courts about the nature of the technology to obtain orders to use it").

Finally, the defense cites to a USA Today article based on two FBI emails regarding the handling of sensitive information. According to the defense, these emails show that the FBI "require[d]" its agents to "withhold information about NITs . . . from prosecutors and case agents." Response at pp. 6-7. The defense argues that these emails are so outrageous that this Court should dismiss "all of the representations" by the FBI in this Motion and the declaration of Special Agent Alfin as "inherently unreliable." *Id.*

The actual emails (assuming they are genuine) show no improper concealment. In the first, an FBI supervisor urges agents not to include sensitive information and details about "trade craft" in internal FBI communications called "ECs." Response, Ex. C-001. Nothing in the email suggests that anyone should be deceived or misled. Rather, the email merely urges the common-sense practice of not disseminating sensitive information unless there is a reason to do so. This concept is called "need to know." It is familiar to anyone who has worked in the military or law enforcement, and it is an entirely proper way to protect sensitive information.

Similarly, the second email (Response, Ex. C-002) addresses the legitimate problem that some of the people who work as prosecutors and agents today will move to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

the private sector in the future. Accordingly, it is common sense not to share sensitive information unless there is a legitimate need to know. Contrary to Michaud's claim, this email does not order the improper concealment of information. Rather, the email ends with a description of the process for getting an AUSA "briefed" on a technical issue. *Id.*

In short, Michaud's argument is outrageous, untrue, and not even supported by the flimsy "evidence" he offers.

C. The government should be permitted to present evidence *ex parte* and *in camera* in order to fully articulate the basis for its claim of a qualified law enforcement privilege.

Turning to the merits of the Motion to Reconsider, the Court should grant the government's request to file a brief *ex parte* and *in camera* so it can fully articulate the basis for its claim of the law enforcement privilege

As an initial matter, it is important to correct Michaud's inaccurate claim that this Court has already denied a request for an *ex parte* submission. In the Response, the defense takes issue with the government's statement that it withdrew its earlier request, and claims that this Court actually "denied the request because the Government had not made any showing of need[.]" The defense offers no cite to the record, however, because none exists. To the contrary, the government agreed to submit a sealed affidavit that was provided to the defense in lieu of an *ex parte* filing. *See* Response, Ex. A, Transcript of February 17. 2015, Hearing at p. 13-15. The Court never ruled on the government's request to submit materials *ex parte*.

Thus, this Court is being called upon to address the propriety of an *ex parte* submission for the first time. That submission would permit the Court to assess that claim of privilege in evaluating the government's motion for reconsideration of its discovery order.

[redacted]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

[redacted]

Rule 16 contemplates exactly the procedure proposed by the government—*i.e.*, providing sensitive information *ex parte* and *in camera*. The Rule states that a court may "for good cause, deny, restrict or defer discovery or inspection[.]" The Rule also specifically authorizes *ex parte* proceedings to establish good cause: "The court may permit a party to show good cause by a written statement that the court will inspect *ex parte*." Fed. R. Crim. Proc. 16(d)(1); *see also United States v. lnnamorati*, 996 F.2d 456, 487 (1st Cir. 1993) ("[Rule] 16(d)(l) expressly authorizes the court to deny discovery of information sought by a defendant based on an *ex parte* showing by the government of the need for confidentiality.").

The Ninth Circuit has held that *ex parte* hearings are permissible under Rule 16. *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998) Indeed, as noted in the government's earlier briefing, such proceedings are routine when a Court is called upon to assess a claim of law enforcement privilege. *See* Dkt. 134, pp. 14-15. Thus, it is entirely appropriate for the government to submit its proposed *ex parte* filing under Rule 16, [redacted]

Michaud disparages *ex parte* proceedings at length in his response. In most cases, all issues can be litigated in full, adversary proceedings. However, there are rare situations where an *ex parte* filing is necessary, and the law [redacted] acknowledges that. The government tried to avoid an *ex parte* filing in this case, and the result was that the Court was not provided with critical information. The proposed *ex parte* filing is meant to correct that error.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Michaud also argues that the FBI's use of NITs, and its penetration of Tor, is so widely known that no sensible criminal would continue to operate on Tor. Response at p. 19. This statement is incorrect, as addressed in the proposed *ex parte* filing.

Finally, Michaud takes the government to task for not at least summarizing the dangers it believes accompany the court-ordered discovery. In truth, Michaud already has a detailed summary of the government's arguments, namely, the government's filings in opposition to the Motion to Compel. In those filings, the government generally discussed—as much as it could in a filing that was not *ex parte*—the sensitive nature of the information at issue and the dangers that disclosure would pose to the interests of law enforcement and national security. [redacted]

As discussed in detail in the proposed *ex parte* filing, the government's concern is not defense counsel's lack of good faith in stating his willingness to honor restrictions on disclosure but the disclosure to anyone at all other than the Court. And the same concern applies to the bases for the government's claim of privilege. Disclosure of that information—even to defense counsel and even under appropriate restrictions—would be nearly as harmful as compliance with the discovery order itself. These matters can only be fully discussed and developed in the *ex parte* filing.

D. Michaud still cannot explain why the discovery he seeks will answer the questions he poses.

With respect to the materiality issue, Michaud cannot explain why the discovery he seeks will help him answer the questions that he claims must be answered. As explained in the government's motion and as Michaud does not contest, he claims he needs the Court-ordered discovery to answer two questions: (1) to verify the accuracy of the information collected and ensure that the NIT did not exceed the scope of the authorizing warrant; and (2) to evaluate the merits of defense theory that someone or something else is responsible for the child pornography found on his devices. Michaud

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

has all he needs to answer both of these questions, and for that reason alone, the Court should grant the government's motion and deny the requested discovery.

As to question one, Michaud has the information collected by the NIT, the computer instructions responsible for collecting that information, and, were he to request it, the network data showing the information collected by the NIT from Michaud's computer and sent to the government. He thus has at his fingertips the code that conducted the "search" of his computer, the "search" results sent to the government by NIT, and the "search" results relied upon by the government in obtaining the warrant for the search its home. If his concern is indeed the scope of the NIT search and the accuracy of the results of that search, he need look no further than what is available to him to allay those concerns.

Michaud cites *United States v. Budziak* as support for his materiality claim. Undoubtedly, *Budziak* involved similar subject matter: that is, a discovery dispute concerning technology used to investigate child pornography offenses. There is a crucial distinction, however. The discovery at issue in that case—related to the peer-to-peer computer program used by law enforcement to download child pornography from the defendant's computer—was critical to the government's proof of distribution counts at trial. *See Budziak*, 697 F.3d 1105, 1111-13 (9th Cir. 2012). The "distribution charge against Budziak was premised on the FBI's use [of a software program] to download files from him" and "[m]uch of the evidence the prosecution presented at trial was devoted to describing" the program and FBI's use of it. *Id*. at 1112. Moreover, "Budziak also identified specific defenses *to the distribution charge* that discovery [regarding the law enforcement program] could potentially help him develop." *Id*. (emphasis added). Thus, it was "logical to conclude that the functions of the program were relevant to his defense." *Id*. That discovery accordingly went to the very heart of the government's proof at trial and the defendant's ability to challenge that proof.

By contrast, on remand, the district court in *Budziak* found—and the Ninth Circuit affirmed—that Budziak had failed to make such a showing regarding a possession count

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

that was unrelated to the use of that software. *United States v. Budziak* ("*Budziak II*"), 612 F. App'x 882, 884-85 (9th Cir. 2015).

The discovery at issue here stands in stark contrast. For Counts 1 and 3 at least—premised on evidence found on the thumb drives and cellular phone seized from Michaud—the disputed discovery is utterly irrelevant to, let alone central to, the government's proof at trial.[3] And even accepting Michaud's flawed premise that he needs the additional discovery to confirm the accuracy of the information collected by the NIT, the most he could hope to do is identify some defect in the information supporting the finding of probable cause authorizing the search of his home. Absent an obvious defect, however, that warrant and the evidence obtained as a result are not open to attack on that basis.

Michaud likewise offers no explanation how the discovery at issue would assist in testing the viability of pressing a defense theory that someone or something else is responsible for the thousands of images of child pornography found on his devices. Instead, he points to news accounts and anecdotal evidence and posits that malicious software *could* expose otherwise innocent computer users to having their devices co-opted by those seeking to store child pornography. As an initial matter, media accounts are hardly competent evidence of technical questions—especially media accounts that have nothing at all to do with the NIT in this case.

Equally unpersuasive is defense counsel's reliance on an unnamed case he tried before Judge Leighton. Although the defense declines to identify the case, it is a matter of public record, *United States v. Lee*, CR04-5281RBL. The defense describes the *Lee* case as an example of how "vulnerabilities" can allow viruses to plant child pornography on the devices of helpless users. The defense highlights the fact that *Lee* was acquitted of

[3] The same cannot be said for Count 2, which is premised on Michaud's activity on Playpen under the username "pewter." As detailed below, the government acknowledges that to the extent the Court does not revisit its prior Order and ultimately concludes that noncompliance by the government warrants a sanction, dismissal of Count 2 may be necessary.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

five counts, which presumably is supposed to show that he was an innocent victim of a virus. Response at p. 10.

The defense's description of *Lee*, however, omits an important fact: Lee was *convicted* of one count of possession of child pornography and sentenced to *fifty-seven months* of imprisonment. CR04-5281RBL, Dkt. 152. This omitted detail demolishes the notion of the *Lee* case as an example of how viruses can "frame" innocent people.

In any event, the key point here is not the flimsy and misleading "evidence" offered by Michaud in support of his virus theory. Rather, the key point is Michaud's inability to explain how the discovery he seeks could shed any light on that theory. Nor does he offer any hint as to why the devices and child pornography found on them do not give him all that he needs to test his theory. Indeed, so far as the government is aware, Michaud has not even attempted to analyze those devices. Surely if the aim is to test the theory that someone or something else is responsible for the highly categorized collection of child pornography found on Michaud's devices, the place to look is the devices and their contents. That Michaud would prefer to look elsewhere is immaterial.

E. Michaud's request for dismissal should be denied as premature, and even if the government's noncompliance with the discovery Order warrants some sanction, a lesser sanction is appropriate.

Michaud's renewed request for dismissal of the indictment should be denied. For starters, the request is premature. The question of what, if any, remedy Michaud is entitled to should the government fail to comply with the Court's discovery order is not yet ripe. Nor will it need to be answered at all should the Court grant the government's motion for reconsideration. For that reason alone, the Court should deny Michaud's dismissal motion so it can be raised when and if doing so is appropriate.

In any event, even if Michaud were entitled to a remedy, dismissal of the entire indictment would be disproportionate given the harm Michaud may suffer if he does not receive the discovery he seeks.

At the outset, it is important to address a defense theme: that the discovery "dilemma" at issue is "one entirely of the Government's own making" because it chose to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

use the NIT to investigate child pornographers on Tor. Response at p. 2. That is an inaccurate and unfair description of the challenges that law enforcement faces when dealing with criminals who use Tor. In truth, the dilemma was created by people like Michaud, who used Tor's anonymity to hide their criminal activity and exploitation of children. As this Court has found, the FBI's use of the NIT was merely an effective response to that dilemma.[4]

Turning to the legal framework, Rule 16 empowers trial courts to manage criminal discovery and enforce the parties' discovery obligations. To accomplish this, a court may "order that party to permit the discovery or inspection; specify its time, place, and manner; and prescribe other just terms and conditions"; "grant a continuance"; "prohibit that party from introducing the undisclosed evidence"; or "enter any other order that is just under the circumstances." Fed. R. Crim. P. 16(d)(2).

It is well settled, however, that when faced with a discovery violation, courts should not impose a sanction harsher than "necessary to accomplish the goals of Rule 16." *United States v. Gee*, 695 F.2d 1165, 1169 (9th Cir. 1983); *cf. United States v. Morrison*, 449 U.S. 361, 364 (1981) (noting in the context of a violation of the defendant's right to counsel "the general rule that remedies should be tailored to the injury suffered from the constitutional violation and should not unnecessarily infringe on competing interests"). The analysis focuses on fashioning a remedy to address actual "prejudice" to the defense. *Morrison*, 449 U.S. at 365. Exclusion of evidence is an "appropriate remedy for a discovery rule violation only where the omission was willful and motivated by a desire to obtain a tactical advantage." *United States v. Finley*, 301 F.3d 1000, 1018 (9th Cir. 2002) (citations and internal quotation marks omitted).

---

[4] Michaud also pillories the government for "boost[ing] the number of visitors" to Playpen during the period the site was under FBI control, claiming that the "only apparent explanation" for this increase is "that the FBI actively redirected people to its site." Response at pp. 24-25. His claim is unsupported, outrageous, and untrue. While it appears that there were more site visits during the two weeks when the FBI had administrative control over the site than estimates of earlier activity on the site, there is no reason to think the FBI's actions had anything to do with it. Nor does Michaud offer any support for such an accusation other than his apparent desire for that to be true. Michaud also insinuates that the government hosted an altered version of the Playpen homepage that made the site appear innocuous. In reality, the FBI merely presented the homepage created by the site administrator.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

In fashioning a remedy for any noncompliance with its discovery order, then, this Court should thus impose a sanction no more severe than is necessary to address the harm resulting from that noncompliance. While the government disagrees that any sanction would be necessary, a sanction far short of dismissal of the entire indictment is all that is required. Specifically, the Court could bar the government from relying on any information the NIT collected from Michaud's computer as evidence at trial. Insofar as the NIT is concerned, prohibiting the government from relying on the information collected by the NIT at trial puts the parties on an even footing. This sanction would also likely result in the dismissal of Count 2 because the evidence supporting that count arises from the Playpen activity of user "pewter." Absent reliance on the NIT information as part of its proof, the government might be unable to attribute this activity to Michaud and thus unable to meet its burden of proof for that count at trial.

As noted above, the evidence supporting Counts 1 and 3—the digital devices and the substantial and organized collection of child pornography found on them—is entirely independent of the NIT. It is true that under normal circumstances, the government's use of the NIT and the fact that it led the government to identify Michaud as a target of its investigation might be a part of the trial presentation. But doing so is not necessary for the government to prove the essential elements of the crime.

To be sure, Michaud will disagree. According to Michaud, it is only with this discovery that he can verify the accuracy of the data collected by the NIT and ensure that NIT did not exceed the scope of the authorizing warrant. However, as noted above, Michaud has at his fingertips the code that generated that data, the network data showing what information was reported by that code, and the information recorded by the government as having been received from Michaud's computer. The discovery he demands will do nothing to further that analysis. Nor does Michaud's other stated reason for needing this discovery—to assess the viability of a defense premised on his having been the victim of a virus or malicious code—alter this analysis. The devices at issue are available to him if he wishes to investigate this theory. His unsupported claim that he

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

should instead be permitted additional discovery entirely unrelated to those devices does not warrant dismissal of the indictment in its entirety.

III. CONCLUSION

For the reasons set forth above, the government respectfully asks this Court to reconsider is discovery order. As noted above, the government believes that Michaud has all tools he needs to address the issues that he claims can only be addressed with additional discovery. To the extent that this Court agrees with this assertion, this Court may grant the motion to reconsider without the need to consider or address the government's proposed *ex parte* filing. Failing that, the Court should nevertheless "deny" production of that information for "good cause" pursuant to Rule 16(d)(1) and permit the government [redacted] in support of its Rule 16(d)(1) argument *ex parte* and *in camera* in order to establish just that.

DATED this 5th day of May, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
MATTHEW P. HAMPTON
HELEN J. BRUNNER
MICHAEL DION
ANDRE M. PENALVER
Assistants United States Attorney
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Telephone: (206) 553-7970
Fax: (206) 553-0755
E-mail: matthew.hampton@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
KEITH A. BECKER
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on May 5, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant. I hereby certify that a copy was served on defense counsel via e-mail.

s/Emily Miller

EMILY MILLER
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-2267
FAX: (206) 553-0755
E-mail: emily.miller@usdoj.gov